Linux Disaster Recovery Best Practices

Continuous Data Protection for Linux and Windows

An R1Soft White Paper

February 15, 2008

Table of Contents

Introduction

There are dozens of articles, websites, and white papers dedicated to disaster recovery "Best Practices," but none cover the superiority of disaster recovery using Linux based software and operating systems. At the forefront of real-time recovery and continuous data backup recovery is R1Soft's Continuous Data Protection (CDP) software that runs on both Linux and Windows. The unique feature of CDP is a Linux system can backup Windows servers without special hardware and complicated configurations.

Since Information Technology (IT) personnel rely on the speed and accuracy of Linux based backup software to quickly restore their systems, R1Soft's CDP products are doing just that – for over 75,000 servers and growing. Disaster recovery requires the right hardware, software, and implementation plan for optimum data recovery. Organizations want to know their systems are safe from natural and human-made disasters. With the right Linux based product from R1Soft, organizations of all sizes can now rely on a solid foundation for disaster recovery "Best Practices" in order to maintain their infrastructure in case of natural or human-made disasters.

Defining Disaster Recovery

Disaster Recovery is the process of instantly rebuilding servers including operating systems, applications, files, and data. A solid disaster recovery plan allows an organization to quickly gain access to data and maintain daily operations. Without a solid plan based on "Best Practices," an organization may never recover from disasters. Worst case scenario, they dissolve or lose millions of dollars in lost revenue, face potential law suits, or risk damage to the organization's reputation.

Issues with Generic "Best Practices"

There are significant issues with the multitude of generic "Best Practices" available on the Internet today. Many of the resources list many complicated steps you need to take in order to protect your systems. Those same resources try to persuade you to spend thousands of dollars on sophisticated hardware. They suggest hiring expensive human resources to develop disaster recovery plans for your organization. If you follow any of those suggestions, you could be left with an expensive bill and you will be missing the most vital component – near continuous data protection.

To sum up the points of the generic "Best Practices" illustrated above, review the following bullet list:

- Complicated steps are needed to develop and implement a disaster recovery plan.
- Expensive unnecessary hardware with sophisticated bells and whistles needs to be in place.
- Expensive human resources for building and implementing hardware and software need to be hired.

- Zero near continuous backup and data recovery are in place.

Implementing a Professional Backup Solution

A solid disaster recovery plan does not require complicated steps, sophisticated equipment, and high dollar human resources. Instead, a simple, yet effective software solution for your existing systems can be installed and configured in less than a day with R1Soft's CDP technology.

CDP Technology

R1Soft's CDP technology will help you be proactive as opposed to reactive and prevent costly data loss. Unlike traditional backup software, there is NO need to first partition your drive and install the operating system. With CDP, you can restore servers directly from disk-based backup. Software can be completely controlled offsite using a web-based interface.

Each recovery point stored on the CDP Server is virtually a complete disk image as seen at a particular point-in-time. Each disk image includes the file system formatting, partition table, and volume management data needed to rebuild the entire disk. R1Soft technology does not require third-party software and runs completely automated based on your specific configuration settings.

CDP technology provides consistent, point-in-time, system-wide backup images. During normal host operation, the R1Soft CDP Agent keeps a journal of disk changes. Incremental backups know what sectors on the disk have changed before the backup operation starts, eliminating the need for file-by-file or block-by-block comparisons for each backup.

Incremental, sector-based backups disregard unused portions of the disk and copy only the disk sectors that have changed since the last backup. When utilized with traditional compression, this feature reduces backup storage by as much as 90% as compared to a traditional system-wide, file-by-file backup.

Linux Disaster Recovery Best Practices Guidelines

Organizations prefer to restore a server using R1Soft versus troubleshooting issues as they occur. The process is much faster and requires little setup time. The guidelines below will help you get the most out of your R1Soft CDP software solution.

1. Determine your recovery method.

There are three methods: 1) Boot CD 2) PXE Boot 3) Live Boot.

Option 1: Linux Boot CD-ROM - A bootable CD ISO is available for download at http://download.r1soft.com/. Burn the ISO image to a CD and boot your Linux Servers from it.

Advantages:
- Easy to use.
- Nothing required other than a Boot CD and CD-ROM.

Disadvantages:
- Requires physical access to the computer to insert the CD-ROM.
- Can not be easily automated or initiated remotely.

Option 2: Linux PXE (network) Boot - A tar.gz file is available for download at http://download.r1soft.com/. Extract this file to your TFTP server. A sample DHCP server configuration is also provided.

Advantages:
- Can be completely automated.
- Requires no physical access.
- Only a working NIC and PXE boot system is required.

Disadvantages:
- Complex to setup. Requires specialized knowledge in setting up and maintaining DHCP and TFTP.
- The DHCP and TFTP server must usually be deployed in the same data center.

Option 3: Linux Live Boot – Linux Live Boot is a self-extract install available for download at http://download.r1soft.com/. Extract this file to a Linux server. A new boot loader (grub or lilo) option will be installed to boot your Linux server directly into disaster recovery mode. An administrator can also initiate a boot into disaster recovery mode via command line.

Advantages:
- Easy to use.
- Great for people renting dedicated servers.
- No physical access is required.
- No PXE boot required.
- Adds a permanent Grub/Lilo boot loader entry for disaster recovery.

Disadvantages:
- System must be accessible over the network and have a working Linux install.
- In most cases, the O/S must first be re-installed before initiating a bare-metal restore. In many cases, this process involves ordering a “restore” from the hosting provider.

2. Determine which servers you are going to use for your backups.

Before you configure your Linux backups using R1Soft, you need to identify the server(s) you plan on using as your backup servers.

3. Test the recovery method you plan on using.

Each of the recovery methods has different advantages and disadvantages. You do not want to be looking through the user's guide or waiting for tech support to reply if you have an emergency.

4. Test boot methods on the different hardware flavors you use.

All three boot methods depend on booting a silver bullet Linux kernel that works on 95% of hardware without any additional settings. Try the disaster recovery boot on the different hardware flavors you use and make sure you have worked out any unexpected issues.

5. Test your network connection.

You may have forgotten how to connect to your network. Or with this particular NIC adapter, you may have to force a switch port to full duplex so you do not get SLOW transfers.

Optional Deployment Solution

Various clients have talked about how they use the R1Soft CDP technology restores as a deployment solution as well. Let's say they have a base box setup and configured the same way they want to deploy ten (10) other boxes of the same configuration. They can use CDP to build servers at the touch of a button. Once a CDP image has been created, users can create as many boxes as needed, at any given time, including scheduled distributions and deployment.

Why Use R1Soft Linux Best Practices

Below are four invaluable features to follow R1Soft Linux Best Practices guidelines.

1. Flexible, Automatic Data Protection Policy

Data on the CDP Server is stored in R1Soft’s patent-pending Disk Safe storage format. Storing the data on disk format enables the CDP Server to archive point-in-time recovery images for long periods of time using as little disk space as possible. A rotation policy can be defined for each configured backup schedule. This policy specifies the number of different incrementals to keep for each schedule and old recovery points are automatically deleted. This flexible system of minutely, hourly, daily, weekly, and monthly recovery point management is capable of meeting a variety of needs.

Please consider the following examples demonstrating the flexibility of the automatic data protection policy:

- synchronize every 10 minutes – retain the last 48 recovery points
- synchronize hourly – retain the last 48 recovery points
- synchronize daily at midnight – retain the last 7 recovery points
- synchronize weekly on Sundays – retain the last 4 recovery points
- synchronize monthly on the 1st – retain the last 48 recovery points

The CDP Server can automatically manage a variety of policies to meet your specific requirements. In addition to policy based management, any unwanted recovery point can be deleted by an administrator at any time. Selected recovery points can also be locked to prevent automatic deletion by a policy.

2. End-To-End Strong Encryption

CDP Server supports strong encryption of disk data using RSA keys and the blowfish cipher. During a synchronization, data is encrypted (and optionally compressed) on the Agent and sent to the server over the network where the data is stored in encrypted form. The data can only be decrypted using an RSA key protected with a passphrase. During a bare-metal restore process, disk sectors are decrypted on-the-fly at the Linux or Windows Agent.

3. High Performance

Sector-based backups increase throughput and reduce overhead. Servers can be fully operational with minimal performance impact during backups. Backups can typically be performed at anytime, even on busy servers.

4. Small Backup Windows

Only changed disk sectors are copied between backups. Incremental backups can be completed in minutes.

The Innovative Standard of Righteous Software

Traditional backup methods typically involve the process of reinstalling the operating system and software applications and then, if possible, restoring the data and settings. With the Righteous Software Backup technology, you will be able to immediately restore your servers directly from disk-based backup without having to first partition your drive and install the operating system.

Complete Linux Disaster Recovery Options

There are many reasons a server can crash. Regardless of the reason, the server must be brought back online in as little time as possible. In the case of disaster or for quick roll-back, your Linux Server can be booted into a special disaster recovery mode. Once

booted into disaster recovery mode, a recovery point can be streamed across the network directly onto your server’s hard disks from the CDP Server.

CDP In-Depth Technical Overview

R1Soft’s Continuous Data Protection Solution is a server software application that enables disk-based data protection and disaster recovery for Linux Servers and work stations running Microsoft Windows and Linux operating systems. CDP Server protects disk volume data using replication and synchronization over the network storing point-in-time snapshots in disk-based storage.

R1Soft’s CDP solution is a near-Continuous Backup system capable of providing hundreds of recovery points per day scheduled as little as 5 or 10 minutes apart. CDP Server works by reading your hard disk volumes at the sector level, bypassing the file system for the ultimate experience in performance and recovery. The disk sector synchronization is performed while the server is online and provides no interruption to other I/O requests even on a busy server. By reading the disk at the lowest possible level, point-in-time recovery images contain your files and all the formatting, partition tables, and volume configuration needed for complete and instant disaster recovery.

The Data Protection Process

Scheduled point-in-time volume snapshots are scheduled on the CDP Server. The CDP server periodically connects to the CDP Agent program and synchronizes changed disk sectors to the CDP Server. The CDP Server creates a new point-in-time image of the disk volume every time it connects to the Agent for synchronization. The point-in-time images are called recovery points and are stored in what Righteous calls a Disk Safe.

Recovery points only consist of a copy of changed disk sectors. Even on very large volumes, disk synchronization typically only takes seconds or minutes to complete. The more frequently recovery points are scheduled the faster they complete. When compression is enabled, hundreds of recovery points can be stored in less space than it takes to store one disk image.

Who is R1Soft?

Founded in 2006, Houston, Texas based R1Soft develops innovative disk based backup products for Linux and Windows servers. Continuous Data Protection (CDP) products deliver nearly continuous data protection, open file backups, bare-metal disaster recovery, and an easy to use web interface. Priced affordably for any sized hosting company, R1Soft makes it possible for every organization to implement and utilize the benefits of a solid backup and recovery system.

Why R1Soft?

R1Soft has become the leader in backup and recovery software solutions. CDP products have been deployed on thousands of servers across the world. Small, medium, and large organizations depend on R1Soft products to automate the demanding tasks of backing up large amounts of data minutely, hourly, daily, weekly, and monthly.

Contact R1Soft Today

To learn more about R1Soft Linux Disaster Recovery and CDP products, visit http://www.r1soft.com or call 1-800-956-6198.